14A.6

OPEN SOURCE TOOLS FOR RISK ANALYSIS AND VULNERABILITY ASSESSMENTS

David Binning, AEM Corporation, Herndon, VA and
A. Coletti*, Syneren Technologies Corp., College Park, MD

1. INTRODUCTION

Focus groups on vulnerability assessments provide nuanced qualitative insights on local priorities but their results are rarely transferable between communities with similar needs because local environmental data sources and models are hard to identify by non-experts.

The alternative approach of performing quantitative assessment where risks are quantified by listing all-hazard consequences and vulnerabilities require in-depth technical knowledge on water systems, and their use remains inaccessible for small communities and businesses.

Open source tools that facilitate access to on-line information sources and numerical models of natural hazards can bridge some of the existing difficulties. An analysis is performed on a sample set of risks to identify the most promising areas where emerging information technologies may find the most advantageous applications.

2. QUANTITATIVE METHOD

In quantitative risk assessment, the total risk of a critical asset or system to a number, N, of threats could be expressed as the sum of the individual risks. Each risk in turn, is the product of the consequence C_i to the system or asset from the results of the threat, the vulnerability of the system or asset, V_i , and the probability of threat, T_i to occur within a given time period (typically 1 year):

1) $\mathbf{R} = \sum_i \; R_i \; = \; \sum_i \; (C_i * V_i * T_i)$ (i = 1, 2, ….N)

Where i is a threat index identifier.

Similarly, the reduction in risk is the benefit achieved from an investments made to reduce the consequences, vulnerability to, or likelihood that the threat will have on the critical asset or system.

This benefit can then be adjusted by the cost to implement the risk reduction measures to produce a series of options that can be prioritized for implementation based on their net-benefit to cost.

Experience with water sector owners and operators undertaking a probability-based risk and resilience assessment of their systems according to a standard like RAMCAP (American Water Works Association, 2010), have repeatedly demonstrated that certain parts of the risk evaluation are straightforward and easy to understand, while others offer an almost insurmountable challenge. Groups of appropriate plant personnel can quickly discuss their systems and come to consensus around:

(a) System Granularity – how detailed does their assessment need to be to achieve usable results. Most groups find that a mix of high-level asset identification mixed with a closer look at sub-systems of critical importance yields a manageable and effective outcome.
(b) Critical Asset Identification – Following a general listing of the assets that make-up the system(s) to be evaluated, most groups are able to quickly identify which of these are critical to the system. Which of the many assets that make-up the system would cause the system to fail and be unable to meet its mission should the asset fail to perform as designed.
(c) Threat Characterization – From their knowledge of the types of natural and man-made threats in the area, the identification of the family of threats that are of most concern to the assessment team is typically not difficult nor time consuming.

On the other end of the assessment difficulty spectrum, most groups in the water sector have experienced varying degrees of difficulty identifying:

(d) Threat Likelihood – The statistical frequency that an identified threat will occur can be daunting for many man-made threats (e.g.

* Corresponding author address: Alex Coletti, Syneren Technology Corp. 4321 Hartwick Rd. College Park, MD 20740; e-mail: acoletti@syneren.com

sabotage, vandalism, terrorist attack). While natural hazard threats are far better documented and hence often have a wealth of past occurrence frequencies, the specter of climate change is calling into question the validity of using historical data as the basis for calculating the recurrence of a natural threat.

(e) Vulnerability Assessment – While assessing the most reasonable consequences from a specific threat can usually be determined, the vulnerability of the asset poses a far more difficult problem for assessment teams. The vulnerability measures the effectiveness of the countermeasures that are (or subsequently will be put) in place to reduce the effects of the threat. Measurements of vulnerability tend to be highly subjective.

2.1 Capturing and Understanding the Data

Overriding the above mentioned challenges faced by those undertaking a risk assessment, is the sheer volume of the data that must be manipulated, stored, displayed, and arrayed in an intelligent and understandable manner.

Without this coherent display, the outcome of the assessment process is a collection of data yielding little real, actionable information. A feeling for the magnitude of the problem can be illustrated by considering a relatively simple system consisting of 10,000 assets of which fully 900 of them are critical to the system's sustained and effective operation. Against these 900, it is easy to assume that fully 50 natural and manmade threats could be arrayed.

Since the basis of the RAMCAP assessment is the requirement that all critical assets be evaluated against all reasonable threats, the analysis immediately starts with 45,000 asset-threat pairs, each requiring analysis, and each producing a specific risk. If each of these systems is subsequently subjected to 2-3 options for reducing the risk (new countermeasures), well in excess of 100,000 risk pairs require analysis. The task can become debilitating.

While filtering and prioritization techniques are powerful tools, far more robust help is required to make sense of the results. The best and most appropriate actions may not always be those that will produce the greatest risk reduction. Risk reduction investments must be balanced with all other operating costs of the system and be incorporated where the greatest return overall can be achieved. Clearly, approaches and tools are needed to assist assessment teams gather the information, assess its appropriateness to the owner's system, see the "big picture" of outcome results, and support decision making by the group. Open-source software tools hold the promise to help corral the data beast that risk assessment creates.

2.2 PARRE™ – An Open Source Tool for Probability Based Assessments

The Program to Aid Risk and Resilience Evaluations (PARRE™) is an open-source software system designed specifically to support probability-based risk and resilience assessments. PARRE uses the RAMCAP approach and is designed to aid the assessment team by helping to capture appropriate data, storing findings, completing the calculations, and guiding the assessment team through the process. This software tool has been Safety Act certified by the Department of Homeland Security for directed threats. The power of the tool is its ability to undertake much of the drudgery of an assessment for the team. However, additional software tools are needed on both the front and back-end of PARRE to help the team capture information and subsequently to display the results to permit decisions to be made.

3. QUALITATIVE METHOD

Deliberative risk ranking assessments performed according to qualitative protocols are performed by focus groups of stakeholders with the help of a group coordinator. The group coordinator ensures that all the stakeholders have the same understanding of the objectives of the meeting and of the vulnerability concept. In addition, he/she assists in defining risks in ways that are clear, unique, and unambiguous.

In qualitative assessments, each individual risk is still evaluated following the same criteria as in Eq. 1, but fuzzy logic like ranges for $\boldsymbol{C_i}$, $\boldsymbol{V_i}$, $\boldsymbol{T_i}$ are pre-defined (e.g. Low, Medium, High for probability **C** or like once a year, every 10 year, or every 100 years for **T**).

Since focus groups typically take into account a limited number of components in a water system, the number of terms in the qualitative assessment equation remains manageable for first approximation risk analysis and high level list of local threat. Additionally, during qualitative assessments relative local experiences are easier to reconcile between groups by accessing information sources they trust.

Due to their broader scope, focus group assessments cannot be easily validated because different groups define probabilities ($\boldsymbol{T_i}$) and consequences ($\boldsymbol{C_i}$) using varieties of scales, quality parameters, and statistics (Florig et al., 2001). Consequently, focus group assessments remain rarely transferrable between locations and systems.

To help minimize these issues of scale and local context, attempts were made to standardize vulnerability assessment protocols and informational background provided to focus groups. Polsky et al (2007) in particular developed and tested a deliberative risk ranking methodology, referred to as the Participatory Vulnerability Scoping Diagram (VSD) that was proven to be capable to create consistent conceptual frameworks and to gather inputs from focus groups in different locations.

The VSD experience opened the opportunity for testing the method on stakeholder's focus groups interested water systems served by very different aquifers located in different climate regions of the US. The tests were conducted in parallel with the development of a Vulnerability Assessment Support System (VASS). VASS supplemented the VSD protocol with on-line access to historical records of natural hazards. The VASS website provided stakeholders with weather information at the regional scale and enabled searches on historical damage and local weather temporal records.

Figure 1 illustrates a diagram of the services provided by the VASS to support the assessment work of stakeholders with verifiable information. In the diagram, the list of the historical local events converges with the list of risks analyzed by the focus group at the moment during the final phase of an assessment. During this phase, water system vulnerabilities are verified against specific past events, and risks are validated against local environmental, economic, and demographic projections.

The VASS experiment demonstrated that:

1. Discrete software tools, user data interfaces, and data visualization methods can be integrated in deliberative risks ranking protocols
2. Data accessibility and graphical user interfaces provide consistently useful references to stakeholders during risk analysis of threats related to natural causes.

Therefore, qualitative risk-ranking approaches can provide managers, policymakers, and stakeholders with:

- Common collaborative platform for discussing vulnerability parameters according facts and data;
- Quality controlled measurements for risk assessments;
- Defined metrics useful for comparing assessments according to standardized data on environmental variables.

4. CONCLUSION

A limited review of quantitative and qualitative risk assessments was made to highlights the major features that differentiate these two methods. The information technologies tools considered (PARRE and VASS), illustrate important aspects of the problem using open source computer packages. The hope is that the strengths of the VASS qualitative assessment can improve a very difficult weakness of the RAMCAP in quantifying such parameters as threat likelihood and vulnerability.

The challenges that remain to be solved are both technical and cultural. Technical solutions are needed in the areas of visualization and risks representation. Information based solutions are needed to bridge different viewpoints and background knowledge of the stakeholders during focus groups meetings.

Future work in the areas of image processing, database management, and semantic web development will likely solve these problems in a near future.

AKNOWLEDEGMENTS

The VASS project was developed entirely at SMRC, Sterling (VA), smrcusa.com, with partial funding from NOAA-CPO.

5. REFERENCES

Coletti, A., P. Howe, B. Yarnal, N. Wood, 2012: "Technical Note: A support system for assessing local vulnerability to weather and climate" Natural Hazards, 65, 999-1008.

Florig, H. K., M. G. Morgan, K. M. Morgan, K. E. Jenni, B. Fischhoff, P. S. Fischbeck, and M. L. DeKay. 2001. A Deliberative Method for Ranking Risks (I): Overview and Test Bed Development. *Risk Analysis* 21 (5):913-913.

Fuchs, S., J. Birkmann, and T. Glade. 2012. 'Vulnerability assessment in natural hazard and risk analysis: current approaches and future challenges '*Nat Hazards,* 64:1969–1975.

Howe, P.D., B. Yarnal, A. Coletti, and N. Wood, 2013*: "The Participatory Vulnerability Scoping Diagram: Deliberative Risk Ranking for Community Water Systems" Annals of the Association of American Geographers, 103, 343-352.*

Polsky, C., R. Neff, and B. Yarnal. 2007. 'Building comparable global change vulnerability assessments: The vulnerability scoping diagram.' *Global Environmental Change* 17 (3-4):472- 485.

American Water Works Association, 2010: *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standards for Risk and Resilience Management of Water and Wastewater Systems.* ANSI /ASME-ITI /AWWA J100-10 (R13) ISBN: 9781583217887

Binning, D., "J100 and the SAFETY Act – What's in it for Me?" Journal AWWA, Vol. 106, No. 12, December 2014.

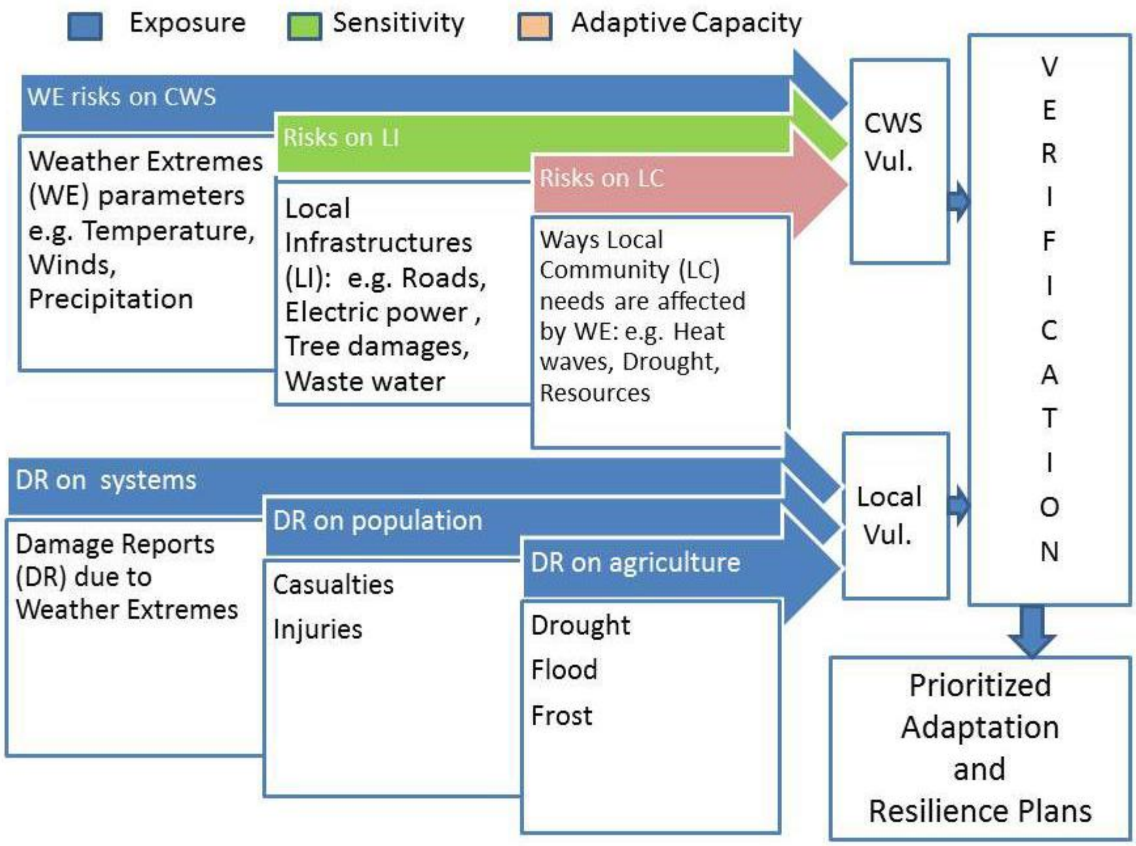

Figure 1: Flowchart of the VASS services from the informational viewpoint developed in the case of community water systems (CWS): users enter and prioritize CWS risks by severity and probability according to their personal experiences of the local weather extremes (WE). Verification of the prioritized vulnerabilities are then provided by the VASS web collaborative environment by displaying list of the available local damage reports (DR-bottom row).